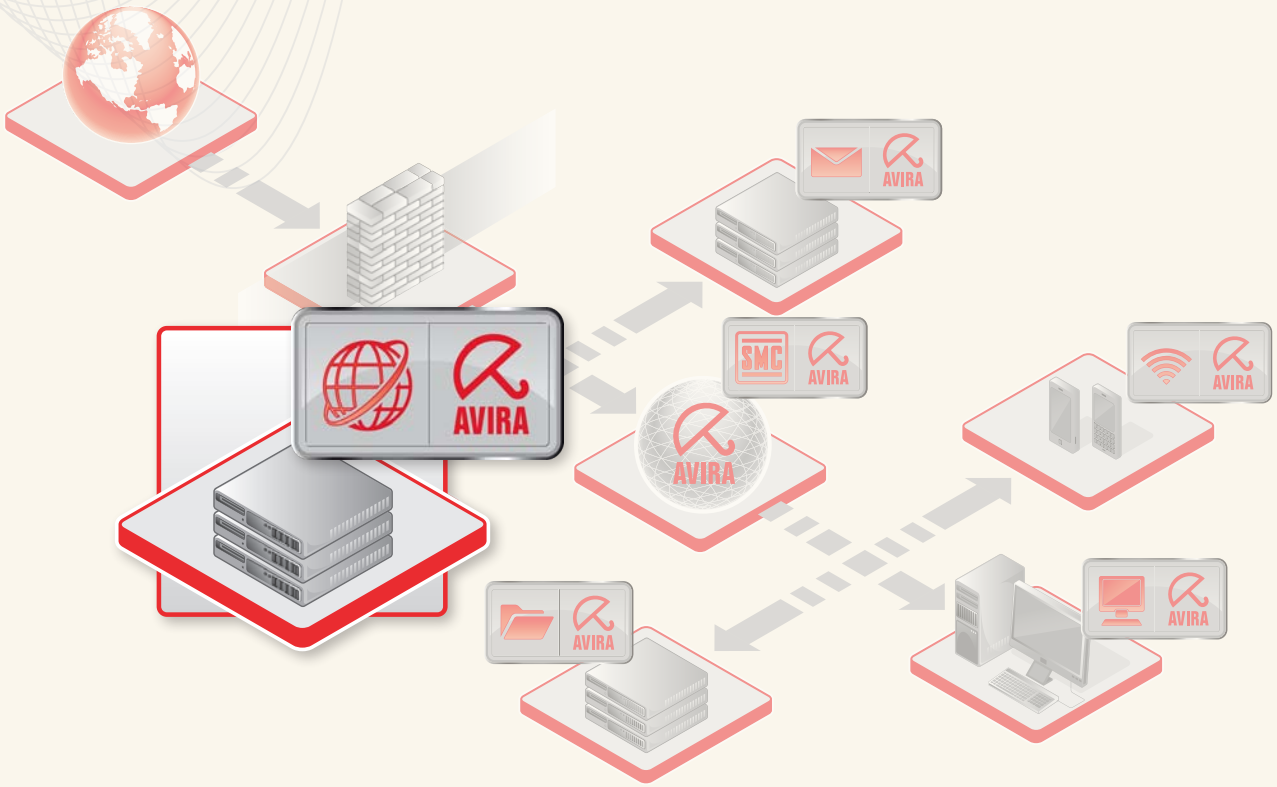
AVIRA
More Than Security

User Manual

# Avira AntiVir ISA Server




www.avira.com

# Table of Contents

# 1 Introduction

The Avira AntiVir ISA Server from Avira GmbH protects your computer against viruses, malware, adware and spyware, unwanted programs and other dangers. This manual deals with viruses and software in brief.

The manual describes the program installation and operation.

Please go to our website at www.avira.com to download the Avira AntiVir ISA Server handbook in PDF form, update the Avira AntiVir ISA Server or renew your license.

You can also find information on our website such as telephone numbers for technical support and information on how to subscribe to our newsletter.

Your Avira GmbH team

# 2 Icons and emphases

The following icons are used:

| Icon | Explanation |
|---|---|
| ✓ | Placed before a condition which must be fulfilled prior to implementation. |
| ▸ | Placed before an action step that you implement. |
| → | Placed before an event that follows the previous action. |
| **Warning** | Placed before a warning of critical vulnerabilities or the danger of data loss. |
| **Note** | Placed before a link to particularly important information or a tip which makes the Avira AntiVir ISA Server easier to use. |

The following emphases are used:

| Emphasis | Explanation |
|---|---|
| *Courier New* | File name or path data. |
| **Bold** | Clicked or displayed software interface elements (e.g. menu item, section or button) |

# 3 Product information

The Avira AntiVir ISA Server is an anti-virus solution specially developed for Microsoft Internet Security and Acceleration (ISA) Servers. The AntiVir ISA Server supports the following Microsoft ISA Servers:

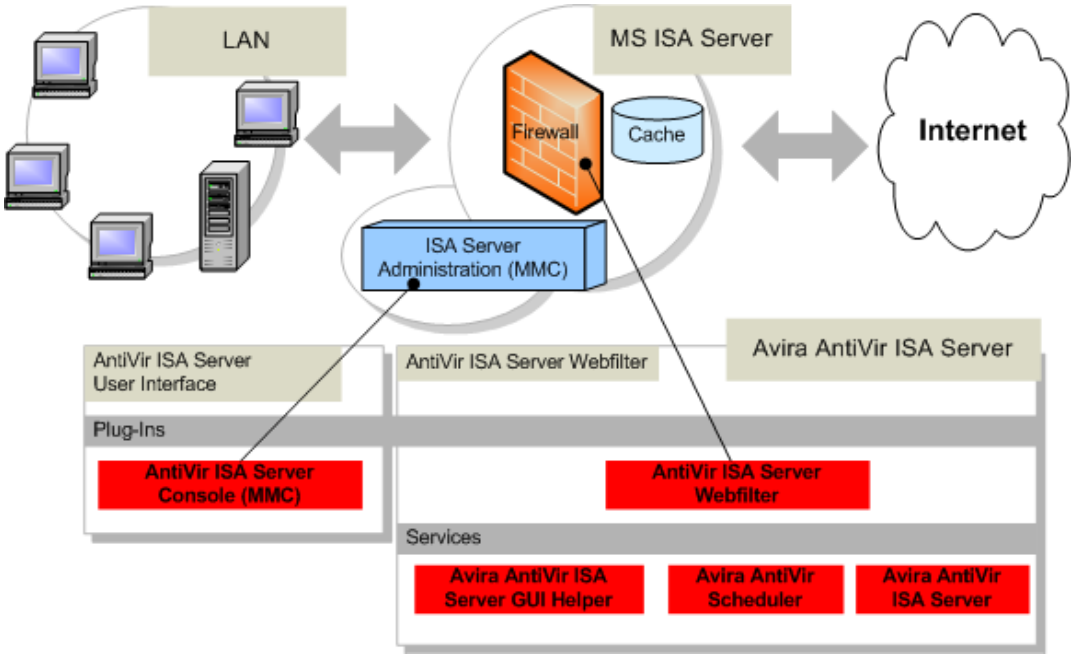
- Microsoft ISA Server 2004 (Standard Edition or Enterprise Edition)
- Microsoft ISA Server 2006 (Standard Edition or Enterprise Edition)

The Microsoft ISA Server integrates a extendable firewall and a web cache (proxy) and can be used as an integrated security gateway in IT environments. The Microsoft ISA Server is designed on the basis of Microsoft Windows security standards and guidelines.

The Avira AntiVir ISA Server scans HTTP data transmitted via the ISA Server for viruses and malware. If a virus is detected, the data transfer is stopped. This helps you protect your business' IT environment and ensure secure access to data and applications.

Note
The HTTPS protocol is not supported at this time, i.e. data sent and received via this protocol has not been scanned for viruses or unwanted programs. Requests via the HTTPS protocol are forwarded transparently. It is therefore also possible to use the Microsoft ® ISA Server for the HTTPS protocol.

### Architecture



The Avira AntiVir ISA Server is integrated into the firewall of the Microsoft ISA Server and the ISA Server Administration via plug-ins. The AntiVir ISA Server Webfilter caches the data transmitted by the ISA Server and forwards requests for virus scans to the Avira AntiVir ISA Server. If a virus is detected, the AntiVir ISA Server Webfilter forwards notifications to the Microsoft ISA Server and the transfer of data to the requesting client is stopped. When viruses are detected, alerts are generated on the Microsoft ISA Server and the requesting clients receive a warning message. The AntiVir ISA Server service scans the data for viruses and malware. To carry out automatic updates, the Avira AntiVir Scheduler service starts the AntiVir ISA Server update process. The Avira AntiVir ISA Server GUI Helper services supports communication between the AntiVir ISA Server User Interface and the components of the AntiVir ISA Server Webfilter.

Use the MS ISA Server Enterprise Edition in cluster operation, install the Avira AntiVir ISA Server module as follows:

- Install the AntiVir ISA Server Webfilter module on all computers that are members of an ISA Server Array.
- Install the AntiVir ISA Server User Interface module on the computer of the MS ISA Server Administration.

## 3.1 Delivery scope

### Features

- Checking of all HTTP and FPT over HTTP data traffic.
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method
- Innovative AHeAD (Advanced Heuristic Analysis and Detection) technology for detection of unknown or fast changing attackers for proactive security
- Browser timeout prevention through browser comforting and progress messages
- Detection of all conventional archive types including detection of nested archives and smart extension detection
- Options for blocking archive bombs
- Individual definition of the scope of scans and options for blocking unwanted content using configurable mime-type filters, file-type filters and URL filters.
- Automatic updates and configurable update cycles
- Consoles for monitoring and configuring AntiVir ISA Servers integrated into the ISA Server Administration (MMC).
- Support for ISA Server Arrays
- Support for ISA Server alert functions

## 3.2 System requirements

The AntiVir ISA Server supports the following Microsoft ISA Servers:

- Microsoft ISA Server 2004 (Standard Edition or Enterprise Edition)
- Microsoft ISA Server 2006 (Standard Edition or Enterprise Edition)

The following system requirements and specifications are required:

AntiVir ISA Server Webfilter:

- Operating system:
  From Windows Server 2003, SP1
- Executable Microsoft ISA Server:

  Microsoft ISA Server 2004 (Standard Edition or Enterprise Edition) or
  Microsoft ISA Server 2006 (Standard Edition or Enterprise Edition)

- Server computer with at least 1500 MHz processor (depending on the number of users)
- At least 512 MB RAM, 1024 MB recommended
- NTFS formatted local partition with at least 150 MB free disk space, additional memory for web-caching content

AntiVir ISA Server user interface:

- Operating system:

  Windows XP (Home or Professional), SP2 or higher or

  Windows Vista or

  From Windows Server 2003, SP1

- Microsoft ISA Server Console:

  Microsoft ISA Server Console 2004 (Standard Edition or Enterprise Edition) or

  Microsoft ISA Server Console 2006 (Standard Edition or Enterprise Edition) or

- .NET Framework 3.5, SP1
- Computer with at least a 400 MHz Pentium processor, 1 GHz recommended
- At least 96 MB RAM, 256 MB recommended

**Note**
The Avira AntiVir ISA Server supports Microsoft ISA Server Enterprise Edition in cluster operation: You can administer the AntiVir ISA Server installed on members of an ISA Server Array in the array.

## 3.3 Licensing

You require a license to use the Avira AntiVir ISA Server. The license is issued in the form of a digital license key in the file hbedv.key. You can obtain the license file by email from Avira GmbH. The license file contains the license for all products that you have ordered in one order process. The Avira AntiVir ISA Server is licensed for each connected client PC. A license pack for the Avira AntiVir ISA Server generally includes licenses for 200 client PCs.

Activate your license for the Avira AntiVir ISA Server with the license file hbedv.key. During the installation process you will be asked to load the license file. To extend your license or load the license after installation, save the license file to the program directory.

# 4 Installation and Uninstallation

## 4.1 Installation

Before installing the AntiVir ISA Server, check the following requirements:

✓ Ensure that the system requirements are met (see System requirements).

✓ Ensure that you are logged in to the computer as an administrator or as a user with administrator rights.

✓ Ensure that an Internet connection exists for updating the AntiVir ISA Server.

✓ Ensure that a valid license file hbedv.key exists and is stored in a local directory on the server.

### Installation types

During installation you can select a setup type in the installation assistant:

Full

The AntiVir ISA Server is fully installed with the AntiVir ISA Server Webfilter and the AntiVir ISA Serve User Interface Console. No destination folder can be selected for the program files to be installed.

User-defined

You can select whether you want to install the Avira AntiVir Server Webfilter and/or the AntiVir ISA Server User Interface Console. A target folder can be selected for the program files to be installed.

### Performing installation

The Avira AntiVir ISA Server is installed as follows:

- Start the installation program by double-clicking on the installation file that you have downloaded from the internet or insert the program CD.
- The installation assistant opens. Follow the instructions of the installation assistant. Complete the following installation steps:
- Confirmation of license agreements
- Selection of setup type (complete installation or custom installation)
- Licensing the AntiVir ISA Server: Load the license file or select the 30 day evaluation license
- Installation of the AntiVir ISA Server Webfilter and/or the AntiVir ISA Server User Interface.

→ The computer needs to be restarted after installation.

After installation, the AntiVir ISA Server Webfilter plug-in is enabled on the ISA Server, the AntiVir ISA Server Webfilter is configured with default settings.

### Update

After installation, the AntiVir ISA Server should be updated: Ensure that the AntiVir ISA Server can receive data from the internet. A proxy server through which the AntiVir ISA Server receives updates can be specified in the AntiVir ISA Server configuration:

- Specify a proxy server for receiving updates under Settings :: Update :: Proxy.

## 4.2 Uninstallation

Uninstallation is carried out via the control panel of the operating system:

- Under Control panel :: Software, find the Avira AntiVir ISA Server and click the **Remove** option.
- Confirm uninstallation.

During uninstallation, AntiVir services are stopped, all program files, configuration files and log files are deleted.

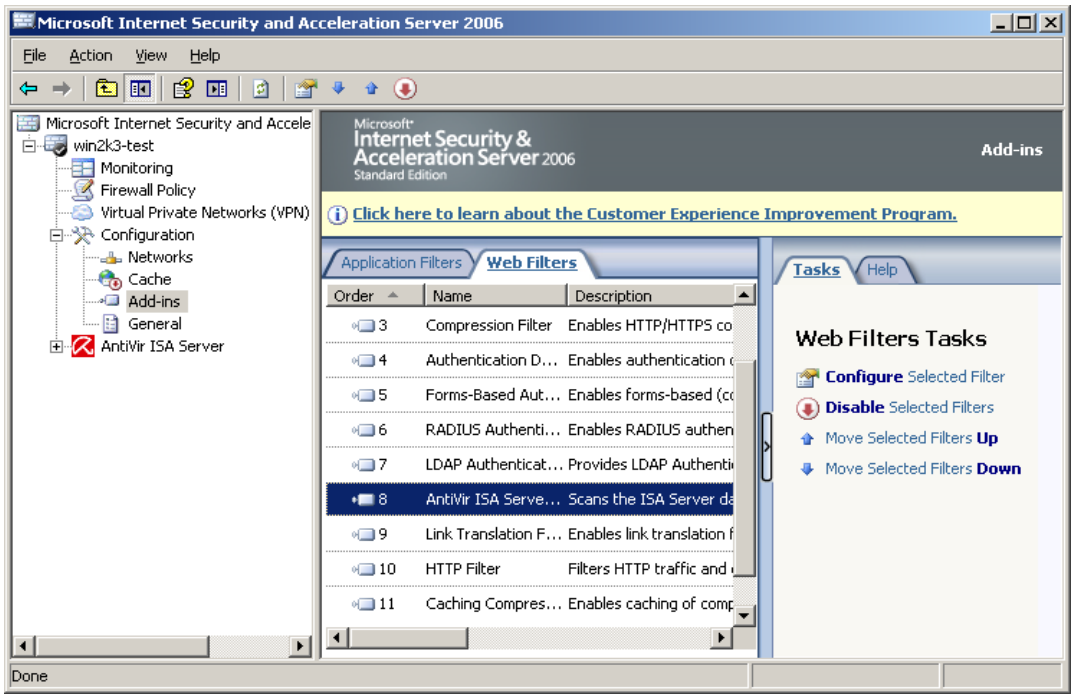
# 5 User interface and operation

The AntiVir ISA Server Webfilter is administered via the AntiVir ISA Server Console. The AntiVir ISA Server Console is integrated in the ISA Server Administration via a plug-in. The ISA Server Administration is a snap-in of the Microsoft Management Console (MMC). If you download the ISA Server Administration, the AntiVir ISA Server Console is included. The administration and configuration of the AntiVir ISA Server is displayed as an individual node on the ISA Server Snap-in Console. The following options for controlling the AntiVir ISA Server are integrated in the ISA Server Administration:

- **Enable and disable**: The AntiVir ISA Server Webfilter plug-in is displayed in the ISA Server Administration under **Configuration :: Add-Ins :: Webfilter**. You can disable or enable the AntiVir ISA Server via the plug-in.
- **Monitoring**: For certain events, individual ISA Server Alerts are generated by the AntiVir ISA Server. The alerts can be called up in the ISA Server Administration under *Monitoring::Alerts*.
- **Administration and Configuration**: The administration and configuration of the AntiVir ISA Server is available as an individual node in the ISA Server Administration on the ISA Server Snap-in Console. Depending on the edition used and the configuration on the ISA Server, the AntiVir ISA Server node is displayed under the ISA Server node or under the ISA Server Array node. You can configure the AntiVir ISA Server for either one ISA Server or for an entire ISA Server Array.

### Enabling and disabling the AntiVir ISA Server via the AntiVir ISA Server Webfilter.

The AntiVir ISA Server Webfilter plug-in is displayed in the ISA Server Administration under **Configuration :: Add-Ins :: Webfilter**. After installation of the AntiVir ISA Server, the AntiVir ISA Server Webfilter is enabled by default.



If you want to enable or disable the AntiVir ISA Server Webfilter:

- Select AntiVir ISA Server Webfilter and under tasks, click configure **Selected filter**.

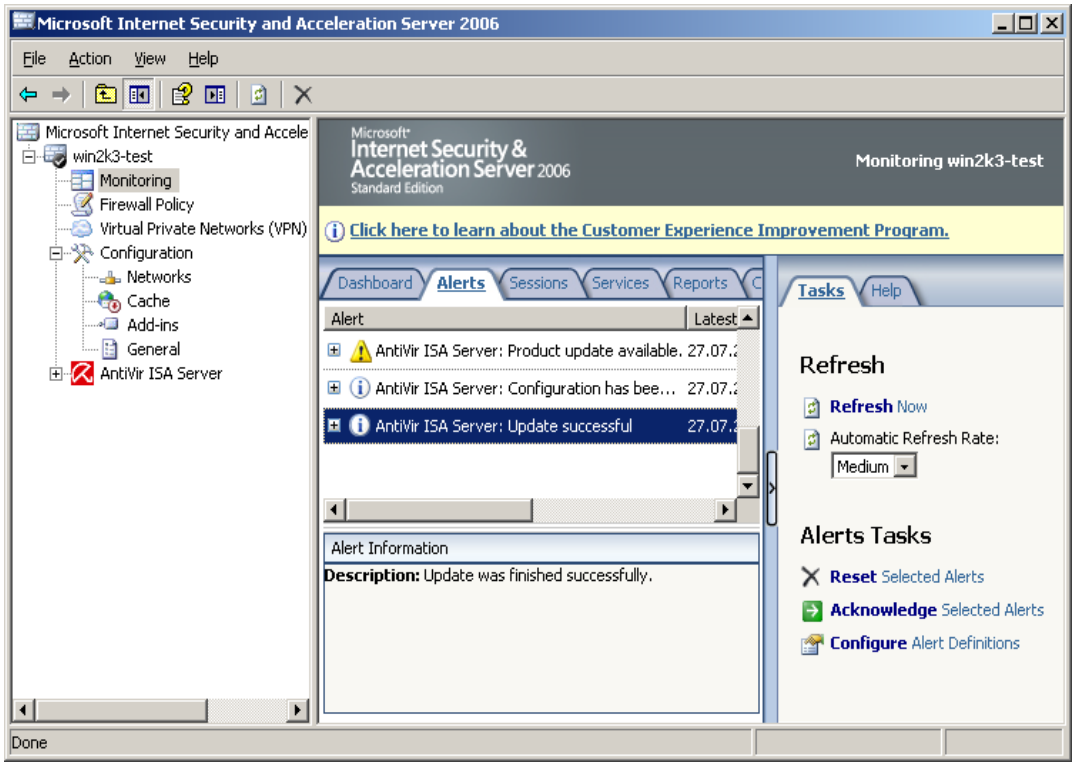
  - OR -

- Selected AntiVir ISA Server Webfilter. Double-click the AntiVir ISA Server Webfilter interface to open.
- If you want to enable the AntiVir ISA Server Webfilter, enable the option *Enable this filter* on the AntiVir ISA Server Webfilter properties page. Confirm your settings by clicking **OK** or **Apply**.
- If you want to disable the AntiVir ISA Server Webfilter, disable the option *Disable this filter* on the AntiVir ISA Server Webfilter properties page. Confirm your settings by clicking **OK** or **Apply**.
- Confirm the configuration changes again using the **Apply** button in the upper bar for accepting changes.

**Warning**
To implement configuration changes, the changes must be confirmed by clicking the **Apply** button in the ISA Server Administration.

## Monitoring the AntiVir ISA Server with ISA Server alerts

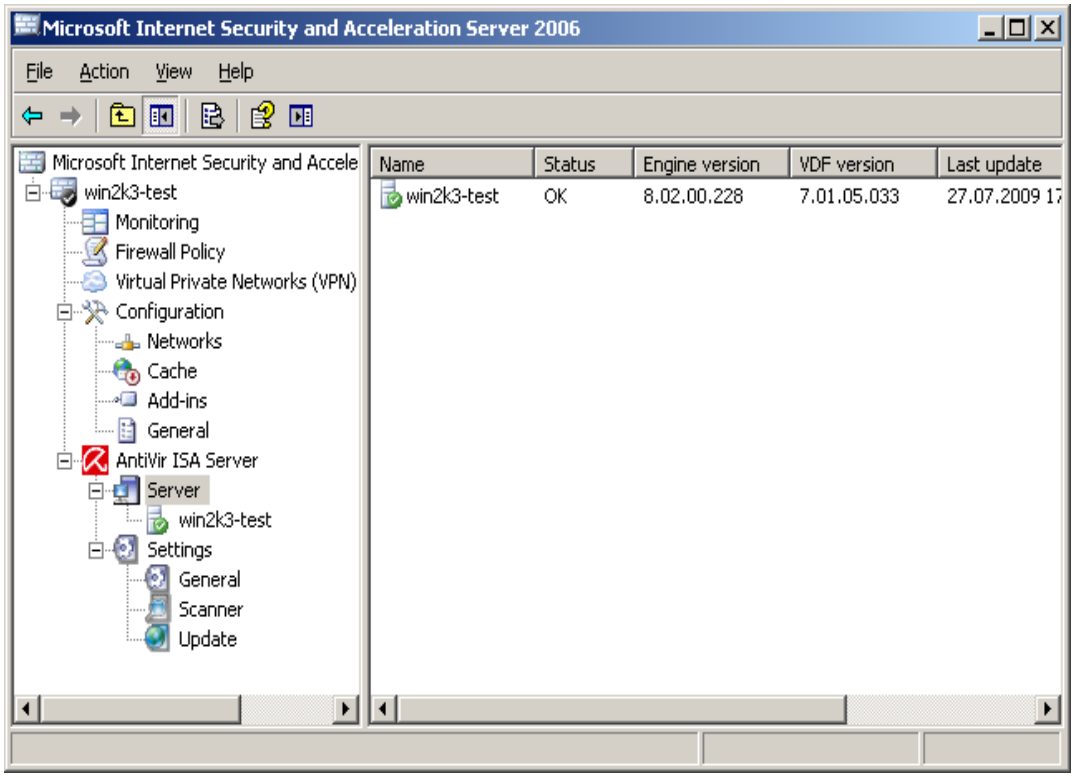
Alerts from the AntiVir ISA Server are displayed in the ISA Server Administration under *Monitoring::Alerts*.




You can open the configuration for ISA Server alerts with the command **Configure alert definitions** under *Alert tasks*. You can define actions for AntiVir ISA Server alerts.

## Administering and configuring the AntiVir ISA Server

The administration and configuration of the AntiVir ISA Server is displayed as an individual node in the ISA Server Administration. All installed AntiVir ISA Servers are displayed together with their status on the Server-Node properties page. You can configure the AntiVir ISA Server on the properties pages for the nodes under settings.




Starting and stopping the AntiVir ISA Server Console

The AntiVir ISA Server Console is integrated into the ISA Server Administration via a plug-in and is started and stopped in the ISA Server Administration..

Operation

- Navigate via the console structure in the left-hand window of the ISA Server Administration. Navigation elements are also displayed as objects on the right-hand properties pages of the ISA Server Administration. Open these objects in the detail window by double-clicking. The AntiVir ISA Server configuration can be found under the settings node. You can select various configuration sections on the Properties page.
- Commands and actions are available via context menus for individual console nodes or objects in the detail window.
- When configuring the AntiVir ISA Server, you must confirm your details by clicking the **Apply** button in the upper bar of the Properties page in order to accept the new settings. To cancel your settings, click the **Cancel** button. The bar for applying changes is displayed automatically as soon as you define your configuration changes.

# 6 Virus detection

When a virus or unwanted program is detected, the data transfer is stopped. The requested data does not reach the client's computer. Date infected by viruses is deleted from the ISA Server. A warning message is displayed in the client's browser:


The AntiVir ISA Server transmits the event and the alert to the ISA Server:

– AntiVir ISA Server: **A virus was found**

# 7 Alerts

AntiVir ISA Server generates alerts on the ISA Server which can be called up under **Monitoring :: Alerts**. The following AntiVir ISA Server alerts are available:

**Error:**

- **AntiVir ISA Server: Error loading configuration data**

  The AntiVir ISA Server was not able to load the configuration data correctly.

- **AntiVir ISA Server: Internal error**

  An internal/unexpected error has occurred.

- **AntiVir ISA Server: Search engine error**

  The AntiVir ISA Server has received an error from the AntiVir Search Engine.

- **AntiVir ISA Server: Update failed**

  Update could not be carried out or was terminated by an error.

- **AntiVir ISA Server: Connection to search engine failed**

  The attempt to create a connection to the AntiVir Search Engine failed..

**Warnings:**

- **AntiVir ISA Server: A virus was found**

  A virus or unwanted program was found in the requested HTTP data..

- **AntiVir ISA Server: Product update available**

  New program files for the AntiVir ISA Server are available for download.

- **AntiVir ISA Server: Virus definition file is out of date**

  The virus definition file is older than the update reminder cycle you have selected (see Settings::General::Warnings) .

**Information:**

- **AntiVir ISA Server: Filter started**

  The AntiVir ISA Server was started.

- **AntiVir ISA Server: Filter stopped**

  The AntiVir ISA Server was stopped.

- **AntiVir ISA Server: Update successful**

The update was carried out completely and without errors.

Actions such as Send email can be configured for the alerts:

- Under**Monitoring:: Alerts :: Tasks** click on **Configure alert definition**.
- Using the *General* tab, select the AntiVir ISA Server alert for which you want to define an action and click **Edit**.
- Using the **Actions** tab, define the actions that should follow the alert.
- Click **Apply** to confirm your settings and close the window by clicking **OK**.

Note
All AntiVir ISA Server alerts are configured by default with the action*Write in Windows Event log*.

**Warning:**
Please note the following when configuring alert definitions: If a particular alert is deleted, it cannot be retrieved. The deleted alert can only be reactivated or recreated by reinstalling the AntiVir ISA Server product. It is therefore recommended that unnecessary alerts are deactivated. (See Microsoft® ISA Server documentation).

# 8 Updates

The effectiveness of anti-virus software depends on how up-to-date the program is, in particular the virus definition file and the search engine. For this reason, regularly download updates for the Avira AntiVir ISA Server from our download servers. To automatically perform regular updates, the Avira AntiVir Scheduler service is integrated into the Avira AntiVir ISA Server.

An update updates the following components:

- Virus definition file
- Search engine
- Program files (product update)

An update checks whether the virus definition file and search engine are up-to-date and if necessary implements an update. Product updates are performed as per the configuration. On the AntiVir ISA Server Console you can start a product update manually in the context menu of a server node. A restart of the system after an update is required only after a product update. By default, the Avira AntiVir Scheduler service starts updates every 10 minutes. You also have the option to configure the update interval.

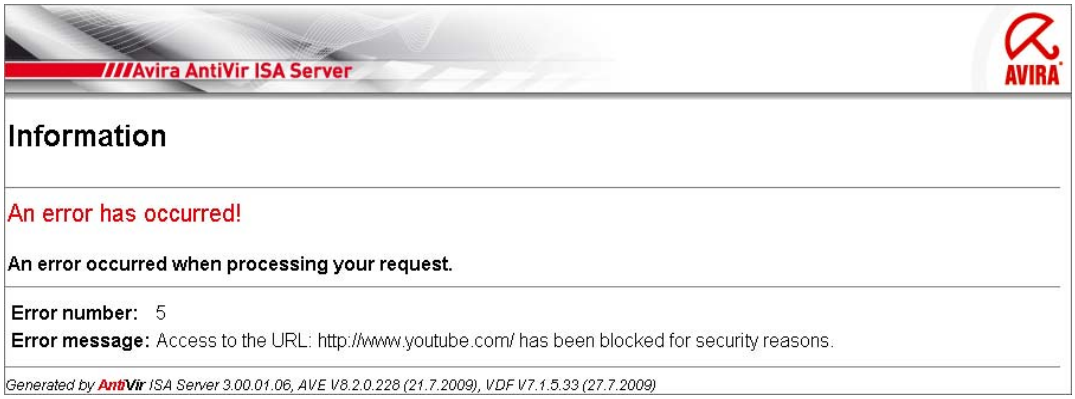
# 9 Client notifications

AntiVir ISA Server scans the HTTP data flow for viruses and malware, stops the transfer of data if a virus is detected and blocks unwanted web content. AntiVir ISA Server clients receive notifications when a virus is detected and when web content is blocked. A download progress bar is generally displayed when downloading larger quantities of data.

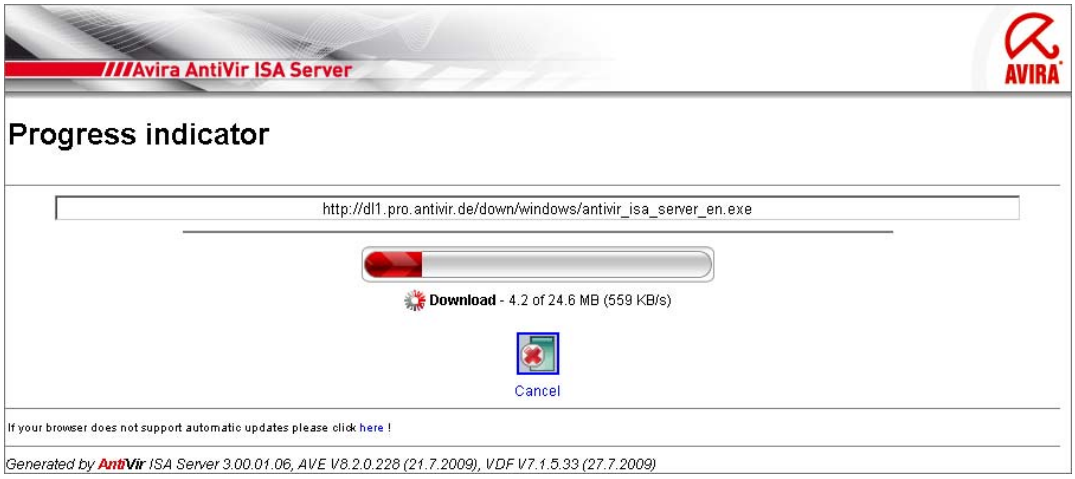
Overview of client notifications:

### Virus detection


### Locked request




### Progress bar when downloading larger quantities of data




When the download to the ISA Server is completed, the data is then scanned by AntiVir ISA Server for viruses and malware. If no viruses or malware are found, the client can begin the download to the client computer via the **Save file** link.

# 10 Configuration options

Under *Settings* you can configure AntiVir ISA Server.

**Note**
Where necessary and depending on which ISA Server Edition you are using and on your system architecture, you can configure an AntiVir ISA Server or an ISA Server Array with multiple AntiVir ISA Servers under Settings. To simplify the description, configuration options documentation refers to **the configuration of AntiVir ISA Server**

The following configuration options are available:

– *General*:

*General*: Basic settings, such as Enabling statistics, Size of output buffer

Extended threat categories: Selection of additional threat categories

*Content delivery*: Limiting value to prevent timeout

*Warnings*: Alert function for Update status

*Report*: Enable, Disable and Scope of log function

– *Scanner*:

*General*: Basic settings, such as Limit values for in-memory scan

*Locked requests*: File types, MIME types, URLs to be blocked

*Exceptions*: File types, MIME types, URLs excluded from the malware scan

*Heuristic*: Enable, Disable macrovirus heuristic, Enable, Disable and Step-by-step regulation of AHeAD technology

*Archives*: Enable and Disable archive scan, Archive scan exceptions

– *Update*:

*Update*: Carry out product updates, Notification of product updates, Update cycle

*Proxy*: Proxy server used for updates

### Save and apply configuration changes

▶ To save changes to the configuration, click the **Apply** button in the upper bar on the Properties pages of the AntiVir ISA Server configuration. The bar for applying changes is displayed automatically as soon as you define your configuration changes.

In the ISA Server Standard Edition it can take a few minutes for the saved configuration to be accepted by the AntiVir ISA Server.

In the ISA Server Enterprise Edition with configuration memory server, the configuration is saved in the configuration memory server and is transmitted to all array members in the configured interval of the configuration memory server.

**Note**
Configuration changes do not require the AntiVir ISA Server service to be restarted.

### Context menu

Restore settings

This command enables you to restore AntiVir ISA Server configuration settings to default values:

# 10.1 General

## 10.1.1 General

The basic settings for AntiVir ISA Server can be defined under *General :: General*

### Settings

Block data access if AntiVir Webfilter not available

If the AntiVir ISA Server Webfilter is not available, access to all data is blocked. Each time a page is requested, the user (client) receives an error message (HTTP status code 502: Bad gateway / Proxy error). The option is enabled as the default setting.

Possible reasons for non-availability of the AntiVir ISA Server Webfilter include:

- The search engine cannot be accessed, e.g. because the license file is invalid.
- The AntiVir ISA Server Webfilter could not be loaded.
- The AntiVir ISA Server service was stopped.

**Note:**
For technical security reasons, it is recommended that this option is enabled.

Collect statistics data

If this option is enabled, statistical data from the AntiVir ISA Server is secured. The statistical data is displayed under *Server* on the node of the corresponding server. The option is enabled as the default setting.

Size of output buffer

You can control the size of the output buffer for each connection with the aid of the slider. The recommended standard value is 2 MB.:

**Note**
Please note that increasing the output buffer for each connection involves significantly increased system memory use.

### SecureNAT client support

Enable SecureNAT client support

When this option is enabled, AntiVir ISA Server supports SecureNAT clients.

**Note**
When there are requests from the SecureNAT client to the web server of AntiVir ISA Server - for example when requesting the content of AntiVir client notifications - the IP address 14.200.200.1 is used as the address of the AntiVir web server.

### 10.1.2 Extended threat categories

By default the AntiVir ISA Server scans data transmitted by the ISA Server for viruses or malware. Under **Extended threat categories** you can select from a list of further threat categories you want the AntiVir ISA Server to capture (see Extended threat categories). The following threat categories are available for selection:

- Dialer (DIALERS)
- Adware/Spyware (ADSPY)
- Application (APPL)
- Backdoor Clients (BDC)
- Games (GAMES)
- Double Extension Files (HEUR-DBLEXT)
- Jokes (JOKES)
- Unusual Runtime Compression Tools (PCK)
- Phishing
- Security Privacy Risk (SPR)

*Enable all*

If this option is enabled, all types are enabled.

### 10.1.3 Content delivery

Under *Content delivery* you can adjust the behavior of the AntiVir ISA Server when downloading larger quantities of data. When downloading larger quantities of data, the data from the AntiVir ISA Server is fully cached on the hard disk before being scanned for viruses and unwanted programs by the AntiVir Search Engine. Some browsers can cause a timeout to occur, followed by an interruption of the download. To ensure content delivery, even for larger quantities of data, the AntiVir ISA Server provides various timeout prevention methods when communicating with the requesting client. In *Content delivery* you can define the limiting values at which the timeout prevention methods are activated.

#### Limiting value to prevent timeout

Activate from file size of n KB

This option enables you to define the file size (KB) at which timeout prevention is activated. The recommended standard value is 4096 KB.

Activate after n secs.

This option enables you to define the number of seconds of download time after which timeout prevention is activated. The recommended standard value is 8 seconds.

**Note**
Timeout prevention is activated when one of the defined limiting values is reached.

**Note**
The AntiVir ISA Server uses the following timeout prevention methods:
Progress bar: The Avira AntiVir ISA Server continuously sends status information for download to the browser (see Ch.. Client Notifications).
Data trickling: The Avira AntiVir ISA Servers continuously sends data to the browser.
Header trickling: The Avira AntiVir ISA Servers continuously sends HTTP header data to the browser. The only function of the header data is to prevent a browser timeout and it is not interpreted by the browser. If you have any questions, please contact Avira GmbH Customer Support. The Customer Support contact information for the relevant server can be accessed in *About*..

### 10.1.4 Warnings

In *Warnings*, you can configure the alert function for the update status of the AntiVir ISA Server.

#### Update

Warning if virus definition older than n days

This option lets you configure the maximum age of the virus definition file in days. If this age is exceeded, an alert is generated on the ISA Server. The following alert is generated using the default alert settings:

- **Alert severity level**: Warning
- **Alert**: AntiVir ISA Server: Virus definition file is out of date.

The recommended default setting for this option is 3 days.

### 10.1.5 Report

Under *Report* you can enable or disable the AntiVir ISA Server logging function (logger) and define the scope of the logger. The log file *avisa.log* is saved in the following directory:

C:\Documents and Settings\All Users\Application data\Avira\AntiVir ISA Server logfiles\

**Note**
The logger of the Update module is limited to 1500 log files and cannot be configured. If the maximum of 1500 log files is reached, each new update deletes the oldest log file.

#### Logging

Off

If this option is enabled, no AntiVir ISA Server actions are logged.

Default

If this option is enabled, only error messages from the AntiVir ISA Server are logged.

Extended

If this option is enabled, error messages and warning messages from the AntiVir ISA Server are logged.

Full

If this option is enabled, all messages and actions of the AntiVir ISA Server are logged.

The log function of the AntiVir ISA Server is disabled by default, as the log function can negatively impact the performance of the ISA Server.

#### Limit report file

Limit size to n KB

If this option is enabled, the report file can be limited to a specific size. This option is activated by default with a value of 1 MB. If the log file exceeds the specified size, the log file entries are backed up in a backup log file and the log file is reset. When the log entries are saved in the backup log file, the entries of the previous backup are overwritten.

## 10.2 Scanner

### 10.2.1 General

Under *Scanner :: General* you can configure the basic settings of the AntiVir ISA Server scanner.

#### Settings

Ignore files larger than n KB

If this option is enabled, files large than the specified value in KB are ignored by the scan module of the AntiVir ISA Server: These files are not scanned for viruses and malware. This option is disabled as the default setting for security reasons. If you enable this option, a value of 10240 KB is recommended.

In-memory scan up n KB

If this option is enabled, files up to the specified size in the ISA Server RAM are scanned for viruses or malware. This option is enabled by default with a value of 512 KB. The in-memory scan enhances the performance of the AntiVir ISA Server.

### 10.2.2 Locked requests

Under **Locked requests** you can specify the file types and MIME types (content types for the transferred data) to be blocked by AntiVir ISA Server. You can block known unwanted URLs, such as phishing and malware URLs. Blocked data is not transmitted from the Internet to the computer systems of ISA Servers (or the computer systems of clients).

#### File types/MIME types to be blocked

Enable

If this option is enabled, all file types and MIME types (content types for the transferred data) on the list are blocked by AntiVir ISA Server.

Input box

In this box, enter the names of the MIME types and file types you want AntiVir ISA Server to block. For file types, enter the file extension with a leading dot, for example, .htm. For MIME types, indicate the media type and sub-type. The two statements are separated from one another by a single slash, e.g. .video/mpeg or audio/x-wav.

**Note**
Files which are already stored on the computer system of the client as temporary internet files and blocked, can however by downloaded locally by the internet browser.

**Note**
The list of blocked file and MIME types is ignored if they are entered in the list of excluded file and MIME types under Settings::Scanner::Exceptions.

**Note**
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

Add

The button allows you to copy MIME and file types from the input field into the list.

Delete

The button removes a highlighted entry from the list.

Examples: File types and MIME types to be blocked

- application/octet-stream = application/octet-stream MIME type files (executable files *.bin, *.exe, *.com, *dll, *.class) are blocked by AntiVir ISA Server.
- application/olescript = application/olescript MIME type files (ActiveX script-files *.axs) are blocked by AntiVir ISA Server.
- ..exe = All files with the extension .exe (executable files) are blocked by AntiVir ISA Server.
- ..msi = All files with the extension .msi (Windows Installer files) are blocked by AntiVir ISA Server.

### URLs to be blocked

Enable

If this option is enabled, all URLs on the list are blocked by AntiVir ISA Server.

Input box

In this box, enter the URLs you want AntiVir ISA Server to block, e.g. **www.domainname.com**. You can specify parts of the URL, using leading or concluding dots to indicate the domain level: .domainname.de for all pages and all subdomains of the domain. Indicate websites with any top-level domain (.com or .net) with a concluding dot: domainname.. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. net for all NET domains (www.domain.net).

**Note**
The list of blocked URLs is ignored if they are entered in the list of excluded URLs under Configuration::Scanner::Exceptions

**Note**
You can also use the wildcard * for any number of characters when specifying URLs. You can also use leading or concluding dots in combination with wildcards to indicate the domain level:
.domainname.*
*.domainname.com
.*name*.com (valid but not recommended)
Specifications without dots, like *name*, are interpreted as part of a top-level domain and are not advisable.

Add

The button allows you to copy the URLs from the input field into the list.

Delete

The button removes a highlighted entry from the list.

Examples: URLs to be blocked

- www.domain.com -OR- www.domain.com/*

  = All URLs with the domain 'www.domain.com' are blocked by AntiVir ISA Server: www.domain.com/en/pages/index.php, www.domain.com/en/support/index.html, www.domain.com/en/download/index.html,..
  URLs with the domain 'www.domain.de are not blocked.

- domain.com -OR- *.domain.com

  = All URLs with the second-level and top-level domain 'domain.com' are blocked by AntiVir ISA Server. The specification implies all existing subdomains for '.domain.com': www.domain.com, forum.domain.com,...

- domain. -OR- *.domain.*

  = All URLs with the second-level domain ’domain’ are blocked by AntiVir ISA Server. The specification implies all existing top-level domains or subdomains for '.domain.’: www.domain.com, www.domain.de, forum.domain.com,...

- .*domain*.*

  All URLs containing a second-level domain with the string 'domain' are blocked by AntiVir ISA Server: www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

- net -ODER- *.net

  = All URLs with the top-level domain ’net’ are blocked by AntiVir ISA Server: www.name1.net, www.name2.net,...

### 10.2.3 Exceptions

In *Exceptions* you can specify the file types and MIME types (content types for transferred data) and URLs to be excluded from the virus and malware scan. The MIME types, file types and URLs specified are ignored by the AntiVir ISA Server, i.e. that data is not scanned for viruses and malware when it is transferred to the client’s computer system.

**Warning**
Certain media formats (streaming content) are excluded from the virus and malware scan by default. If you have any questions, please contact Avira GmbH Customer Support. The Customer Support contact information for the relevant server can be accessed in About.

### Excluded file types / MIME types

Enable

If this option is enabled, all file types and MIME types (content types for transferred data) on the list are excluded from the AntiVir ISA Server scan.

Input box

In this box you can input the name of the MIME types and file types to be excluded from the AntiVir ISA Server scan. For file types, enter the file extension with a leading dot, for example, .htm. For MIME types, indicate the media type and sub-type. The two statements are separated from one another by a single slash, e.g. .video/mpeg or audio/x-wav.

**Note**
No wildcards (* for any number of characters or ? for a single character) can be used when entering file types and MIME types.

**Warning**
All file types and content types on the exclusion list are sent to the client without further scanning of the locked requests (list of file and MIME types to be blocked in Settings::Scanner::Locked requests) For all entries on the exclusion list, the entries on the list of file and MIME types to be blocked are ignored. No scan for viruses and malware is carried out.

Add

The button allows you to copy MIME and file types from the input field into the list.

Delete

The button removes a highlighted entry from the list.

Examples: Excluded file and MIME types

- application/octet-stream = application/octet-stream MIME type files (executable files *.bin, *.exe, *.com, *dll, *.class) are excluded from the AntiVir ISA Server scan.
- application/olescript = application/olescript MIME type files (ActiveX script-files *.axs) are excluded from the AntiVir ISA Server scan.
- ..exe = All files with the extension .exe (executable files) are excluded from the AntiVir ISA Server scan.
- .msi = All files with the extension .msi (Windows Installer files) are excluded from the AntiVir ISA Server scan.

### Skipped URLs

Enable

If this option is enabled, all URLs on the list are excluded from the AntiVir ISA Server scan.

Input box

In this box you can input the URLs to be excluded from the AntiVir ISA Server scan, e.g. **www.domainname.com**. You can specify parts of the URL, using leading or concluding dots to indicate the domain level: .domainname.de for all pages and all subdomains of the domain. Indicate websites with any top-level domain (.com or .net) with a concluding dot: domainname.. If you indicate a string without a leading or concluding dot, the string is interpreted as a top-level domain, e.g. net for all NET domains (www.domain.net).

**Note**
You can also use the wildcard * for any number of characters when specifying URLs. You can also use leading or concluding dots in combination with wildcards to indicate the domain level:
.domainname.*
*.domainname.com
.*name*.com (valid but not recommended)
Specifications without dots, like *name*, are interpreted as part of a top-level domain and are not advisable.

**Warning**
All websites on the list of excluded URLs are sent to the client without further scanning by the AntiVir ISA Server: Blocked URLs are ignored if they are entered in the list of excluded URLs under Settings::Scanner::Locked requests). No scan for viruses and malware is carried out. Only trusted URLs should therefore be excluded from the AntiVir ISA Server scan.

Add

The button allows you to copy the URLs from the input field into the list.

Delete

The button removes a highlighted entry from the list.

Examples: Skipped URLs

- www.domain.com -OR- www.domain.com/*

  = All URLs with the domain 'www.domain.com' are excluded from the virus and malware scan: www.domain.com/en/pages/index.php, www.domain.com/en/support/index.html, www.domain.com/en/download/index.html,..
  URLs with the domain 'www.domain.de' are not excluded from the AntiVir ISA Server scan.

- domain.com -OR- *.domain.com

  = All URLs with the second-level and top-level domain ‘domain.com' are excluded from the virus and malware scan. The specification implies all existing subdomains for '.domain.com': www.domain.com, forum.domain.com,...

- domain. -OR- *.domain.*

  = All URLs with the second-level domain ‘domain.com' are excluded from the AntiVir ISA Server scan. The specification implies all existing top-level domains or subdomains for '.domain.’: www.domain.com, www.domain.de, forum.domain.com,...

- .*domain*.*

  = All URLs containing a second-level domain with the string 'domain' are excluded from the virus and malware scan: www.domain.com, www.new-domain.de, www.sample-domain1.de, ...

- net -ODER- *.net

= All URLs with the top-level domain ‘net’ are excluded from the virus and malware scan: www.name1.net, www.name2.net,...

**Warning**
Enter the URLs you want to exclude from the AntiVir ISA Server scan as precisely as possible. Avoid specifying an entire top-level domain or parts of a second-level domain because there is a risk that Internet pages that distribute malware and undesirable programs will be excluded from the AntiVir ISA Server scan through global specifications under exclusions. You are recommended to specify at least the complete second-level domain and the top-level domain: domainname.com

## 10.2.4 Heuristic

This configuration section contains the settings for the heuristic of the AntiVir ISA Server search engine.

AntiVir ISA Server contains very powerful heuristics that can proactively uncover unknown malware, i.e. before a special virus signature to combat the damaging element has been created and before a virus definition file update is available. Virus detection involves an analysis and investigation of the affected codes for functions typical of malware. If the code being scanned exhibits these characteristic features, it is reported as being suspicious (heuristic hits). This does not necessarily mean that the code is in fact malware. False positives do sometimes occur. Heuristic hits are treated like viruses that have been detected from a known virus signature: The affected data is not sent to the client, a warning message is displayed in the client browser, and an alert is generated on the ISA Server.

### Macrovirus heuristic

**Activate macrovirus heuristic**

If this option is enabled, the heuristic scan for macroviruses is enabled. If the affected data can be repaired, all macros are deleted, and data transfer to the requesting client is authorized. If repair is not possible, all data is treated as viruses.

### Advanced Heuristic Analysis and Detection (AHeAD)

**Enable AHeAD**

If this option is enabled, the heuristic scan for viruses using AntiVir AHeAD technology is enabled. For heuristic hits, the affected data is treated as viruses. You can define how 'sharp’ you want the heuristics to be. The option is enabled as the default setting.

**Low detection level**

If this option is enabled, AntiVir ISA Server detects slightly less unknown malware, the risk of false alerts is low in this case.

**Medium detection level**

This setting optimizes the ratio of detection performance to false positives: If the detection rate of unknown malware is relatively high, relatively few false positives are received. This option is enabled as the default setting and is recommended.

**High detection level**

If this option is enabled, AntiVir ISA Server identifies far more unknown malware, but you must also accept that there are likely to be false positives.

## 10.2.5 Archives

You can adjust the scan for viruses and malware under *Archives*.

### Archive settings

#### Scan archive

If this option is enabled, archives are scanned for viruses and malware by the AntiVir ISA Server. The option is enabled as the default setting.

**Note**
Please note that this functionality can use a lot of computer capacity. If the archive scan is enabled, it is therefore recommended that the recursion depth is limited.

#### Smart extensions

If this option is enabled, the AntiVir ISA Server archive scan detects whether a file is a packed file format (archive), even if the file extension differs from the usual extensions, and scans the archive. Each file must be opened to check the file format. This slows the scan speed. This setting is activated by default and is recommended.

### Exceptions

Under **Exceptions** you have the option of limiting the archive scan. The purpose of archive scan exceptions is to prevent possible system overloads due to archive bombs. If you use the options for limiting the archive scan, it is recommended that the option **block unscanned archives** is enabled. The options for limiting the archive scan are automatically disabled as soon as you disable the option **Scan archives**.

#### block unscanned archives

If this option is enabled, archives that have not been scanned for viruses or malware are automatically blocked by the AntiVir ISA Server. Clients receive a warning message. This option is enabled as the default setting and is recommended.

#### Maximum recursion depth

When scanning archives, the AntiVir ISA Server uses a recursive scan: Archives within archives are unpacked and scanned for viruses and unwanted programs. If this option is enabled, the recursive scan is restricted to the specified maximum recursion depth value. The option is enabled as the default setting.

Archives that exceed the specified maximum value are not scanned for viruses or malware. If the option **block unscanned archives** is disabled, the archive data is transferred to the client unscanned.

You can define the maximum recursion depth for the recursive scan. The recommended standard value is 20: An archive is unpacked up to 19 times and scanned for viruses and unwanted programs.

#### Maximum compression rate (ratio)

If this option is enabled, the archive scan is restricted to a maximum compression rate. The compression rate is defined as the ratio of the original file size to the compressed file size. Archives that exceed the specified maximum value are not scanned for viruses or malware. If the option **block unscanned archives** is disabled, the archive data is transferred to the client unscanned. The option is disabled as the default setting.

#### Maximum unpacked size of archives to be scanned

You can specify a maximum archive size in MB up to which the archives should be scanned. If this option is enabled, archives that exceed the specified maximum value are not scanned for viruses or malware. If the option **block unscanned archives** is disabled, the archive data is transferred to the client unscanned. The option is disabled as the default setting.

# 10.3 Updates

## 10.3.1 Update

In *Update* you can define product update settings and modify the update cycle.

### Product updates

**Automatically download and install product updates**

If this option is enabled, available product updates are automatically installed: The new available program files are downloaded and automatically installed. The option is disabled as the default setting. An open connection to a download server is required to implement this option.

**Warning**
Please note that after a product update, an automatic system restart may be necessary.

**Notify when new product updates are available (recommended)**

If this option is enabled, you will be notified when new product updates become available: The product update icon is displayed on the interface of the AntiVir ISA Server under *Server* and an alert is generated on the ISA Server. The option is enabled as the default setting. An open connection to a download server is required to implement this option. When a product update is available, the following alert is generated using the default alert settings:

- **Alert severity level**: Warning
- **Alert**: AntiVir ISA Server: Product update available

### Scheduler

**Regular updates every n minutes**

With this option, you can configure the update cycle of the AntiVir ISA Server. The recommended standard value is 10 minutes: Every 10 minutes, the virus definition file and the search engine are updated and the system checks if a product update is available. The execution of a product updates depends on the product update settings. An open connection to a download server is required to implement this option.

## 10.3.2 Proxy

Under *Proxy*, you can specify a proxy server with which to create the connection to the Avira GmbH web server.

## Proxy server

### Do not use a proxy server

If this option is enabled, your connection to the web server is not carried out via a proxy server.

### Use Windows system settings

When the option is enabled, the current Windows system settings are used for the connection to the web server via a proxy server.

### Use the following proxy server

If your web server connection is set up via a proxy server, you can enter the relevant information here.

#### Address

Please enter the URL or the IP address of the proxy server you want to use to connect to the web server.

#### Port

Please enter the port number of the proxy server you want to use to connect to the web server.

#### Login name

Enter your login name on the proxy server here.

#### Login password

Enter the relevant password for logging in on the proxy server here.

**Note**
The login password is restricted to 39 characters.

# 11 Viruses and more

## 11.1 Extended threat categories

### Dialer (DIALERS)

Certain services available in the internet have to be paid for. They are invoiced in Germany via dialers with 0190/0900 numbers (or via 09x0 numbers in Austria and Switzerland; in Germany, the number is set to change to 09x0 in the medium term). Once installed on the computer, these programs guarantee a connection via a suitable premium rate number whose scale of charges can vary widely.

The marketing of online content via your telephone bill is legal and can be of advantage to the user. Genuine dialers leave no room for doubt that they are used deliberately and intentionally by the user. They are only installed on the user's computer subject to the user's consent, which must be given via a completely unambiguous and clearly visible labeling or request. The dial-up process of genuine dialers is clearly displayed. Moreover, genuine dialers tell you the incurred costs exactly and unmistakably.

Unfortunately there are also dialers which install themselves on computers unnoticed, by dubious means or even with deceptive intent. For example they replace the internet user's default data communication link to the ISP (Internet Service Provider) and dial a cost-incurring and often horrendously expensive 0190/0900 number every time a connection is made. The affected user will probably not notice until his next phone bill that an unwanted 0190/0900 dialer program on his computer has dialed a premium rate number with every connection, resulting in dramatically increased costs.

We recommend that you ask directly your telephone provider to block this number range to be immediately protected against undesired dialers (0190/0900 dialers).

### Games (GAMES)

There is a place for computer games - but it is not necessarily at work (except perhaps in the lunch hour). Nevertheless, with the wealth of games downloadable from the internet, a fair bit of mine sweeping and Patience playing goes on among company employees and civil servants. You can download a whole array of games via the Internet. Email games have also become more popular: numerous variants are circulating, ranging from simple chess to "fleet exercises" (including torpedo combats): The corresponding moves are sent to partners via email programs, who answer them.

Studies have shown that the number of working hours devoted to computer games has long reached economically significant proportions. It is therefore not surprising that more and more companies are considering ways of banning computer games from workplace computers.

### Jokes (JOKES)

Jokes are merely intended to give someone a fright or provide general amusement without causing harm or reproducing. When a joke program is loaded, the computer will usually start at some point to play a tune or display something unusual on the screen. Examples of jokes are the washing machine in the disk drive (DRAIN.COM) or the screen eater (BUGSRES.COM).

But beware! All symptoms of joke programs may also originate from a virus or Trojan. At the very least users will get quite a shock or be thrown into such a panic that they themselves may cause real damage.

### Security Privacy Risk (SPR)

Software that maybe is able to compromise the security of your system, initiate unwanted program activities, damage your privacy or spy out your user behavior and might therefore be unwanted.

### Backdoor Clients (BDC)

In order to steal data or manipulate computers, a backdoor server program is smuggled in unknown to the user. This program can be controlled by a third party using backdoor control software (client) via the internet or a network.

### Adware/Spyware (ADSPY)

Software that displays advertising or software that sends the user's personal data to a third party, often without their knowledge or consent, and for this reason may be unwanted.

### Unusual Runtime Compression Tools (PCK)

Files that have been compressed with an unusual runtime compression tool and that can therefore be classified as possibly suspicious.

### Double Extension Files (HEUR-DBLEXT)

Executable files that hide their real file extension in a suspicious way. This camouflage method is often used by malware.

### Phishing

Phishing, also known as *brand spoofing* is a clever form of data theft aimed at customers or potential customers of Internet service providers, banks, online banking services, registration authorities.
When submitting your email address on the Internet, filling in online forms, accessing newsgroups or websites, your data can be stolen by "Internet crawling spiders" and then used without your permission to commit fraud or other crimes.

### Application (APPL)

The term APPL refers to an application which may involve a risk when used or is of dubious origin.

## 11.2 Viruses and other malware

### Adware

Adware is software that presents banner ads or in pop-up windows through a bar that appears on a computer screen. These advertisements usually cannot be removed and are consequently always visible. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

### Backdoors

A backdoor can gain access to a computer by going around the computer access security mechanisms.

A program that is being executed in the background generally enables the attacker almost unlimited rights. User's personal data can be spied with the backdoor's help, but are mainly used to install further computer viruses or worms on the relevant system. The connection data allow many conclusions on the usage behavior and are problematic in terms of data security.

### Boot viruses

The boot or master boot sector of hard disks is mainly infected by boot sector viruses. They overwrite important information necessary for the system execution. One of the awkward consequences: the computer system cannot be loaded any more...

### Bot-Net

A Bot-Net is defined as a remote network of PCs (on the Internet), which is composed of bots that communicate with each other. A Bot-Net can comprise a collection of cracked machines running programs (usually referred to as worms, Trojans) under a common command and control infrastructure. Bot-Nets serve various purposes, including Denial-of-service attacks etc., partly without the affected PC user's knowledge. The main potential of Bot-Nets is that the networks can achieve dimensions on thousands of computers and its bandwidth sum bursts most conventional Internet accesses.

### Exploit

An exploit (security gap) is a computer program or script that takes advantage of a bug, glitch or vulnerability leading to privilege escalation or denial of service on a computer system. One form of exploitation for example is an attack from the Internet with the help of manipulated data packages. Programs can be infiltrated in order to obtain higher access.

### Hoaxes

For several years, internet and other network users have received alerts about viruses that are purportedly spread via email. These alerts are spread per email with the request that they should be sent to the highest possible number of colleagues and to other users, in order to warn everyone against the "danger".

### Honeypot

A honeypot is a service (program or server) installed in a network. It has the function to monitor a network and to protocol attacks. This service is unknown to the legitimate user - because of this reason he is never addressed. If an attacker examines a network for the weak points and uses the services which are offered by a Honeypot, it is logged and an alert is triggered.

### Macro viruses

Macro viruses are small programs that are written in the macro language of an application (e.g. WordBasic under WinWord 6.0) and that can normally only spread within documents of this application. Because of this, they are also called document viruses. In order to be active, they need that the corresponding applications are activated and that one of the infected macros has been executed. Unlike "normal" viruses, macro viruses consequently do not attack executable files but they do attack the documents of the corresponding host-application.

### Pharming

Pharming is a manipulation of the host file of web browsers to divert enquiries to spoofed websites. This is a further development of classic phishing. Pharming fraudsters operate their own large server farms on which fake websites are stored. Pharming has established itself as an umbrella term for various types of DNS attacks. In the case of a manipulation of the host file, a specific manipulation of a system is carried out with the aid of a Trojan or virus. The result is that the system can now only access fake websites, even if the correct web address is entered.

### Phishing

Phishing means angling for personal details of the Internet user. Phishers generally send their victims apparently official letters such as emails that are intended to induce them to reveal confidential information to the culprits in good faith, in particular user names and passwords or PINs and TANs of online banking accounts. With the stolen access details, the phishers can assume the identities of the victims and carry out transactions in their name. What is clear is that banks and insurance companies never ask for credit card numbers, PINs, TANs or other access details by email, SMS or telephone.

### Polymorph viruses

Polymorph viruses are the real masters of disguise. They change their own programming codes - and are therefore very hard to detect.

### Program viruses

A computer virus is a program that is capable of attaching itself to other programs after being executed and cause an infection. Viruses multiply themselves unlike logic bombs and Trojans. In contrast to a worm, a virus always requires a program as host, where the virus deposits its virulent code. The program execution of the host itself is not changed as a rule.

### Rootkit

A rootkit is a collection of software tools that are installed after a computer system has been infiltrated to conceal logins of the infiltrator, hide processes and record data - generally speaking: to make themselves invisible. They attempt to update already installed spy programs and reinstall deleted spyware.

### Script viruses and worms

Such viruses are extremely easy to program and they can spread - if the required technology is on hand - within a few hours via email round the globe.

Script viruses and worms use one of the script languages, such as Javascript, VBScript etc., to insert themselves in other, new scripts or to spread themselves by calling operating system functions. This frequently happens via email or through the exchange of files (documents).

A worm is a program that multiplies itself but that does not infect the host. Worms can consequently not form part of other program sequences. Worms are often the only possibility to infiltrate any kind of damaging programs on systems with restrictive security measures.

### Spyware

Spyware are so called spy programs that intercept or take partial control of a computer's operation without the user's informed consent. Spyware is designed to exploit infected computers for commercial gain.

### Trojan horses (short Trojans)

Trojans are pretty common nowadays. We are talking about programs that pretend to have a particular function, but that show their real image after execution and carry out a different function that, in most cases, is destructive. Trojan horses cannot multiply themselves, which differentiates them from viruses and worms. Most of them have an interesting name (SEX.EXE or STARTME.EXE) with the intention to induce the user to start the Trojan. Immediately after execution they become active and can, for example, format the hard disk. A dropper is a special form of Trojan that 'drops' viruses, i.e. embeds viruses on the computer system.

### Zombie

A Zombie-PC is a computer that is infected with malware programs and that enables hackers to abuse computers via remote control for criminal purposes. On command, the affected PC starts denial-of-service (DoS) attacks, for example, or sends spam and phishing emails.

# 12 Info and Service

## 12.1 Contact

If you have any questions or requests concerning the Avira AntiVir ISA Server product range, we will be pleased to help. You can find our contact addresses on the AntiVir Server Console under Server::[server name]::About.

## 12.2 Technical Support

Avira AntiVir ISA Server Support provides reliable assistance in answering your questions or solving a technical problem.

You can find Customer Support addresses from which you can access our comprehensive support services on the AntiVir ISA Serve Console under Server::[server name]::About.

So that we can provide you with fast, reliable help, you should have the following information ready:

- **License information:** You can find license information in your product order documents.
- **Version information:** Version information is displayed on the AntiVir Server Console under Server::[Server-Name]::Version information.
- **Operating system version** and any Service Packs installed.
- **Installed software packages**, e.g. anti-virus software of other vendors.
- **Exact messages** of the program or messages in log files (Report).

## 12.3 Suspicious file

Viruses that may not yet be detected or removed by our products or suspect files can be sent to us. We provide you with several ways of doing this.

- Send the relevant file, packed (WinZIP, PKZip, Arj etc.), as an email attachment to virus@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).
- You can also send us the suspicious file via our website.

## 12.4 Reporting false positives

If you believe that Avira AntiVir ISA Server is reporting a detection in a file that is most likely "clean", send the relevant file packed (WinZIP, PKZip, Arj etc.) as an email attachment to virus@avira.com. As some email gateways work with anti-virus software, you should also provide the file(s) with a password (please remember to tell us the password).

## 12.5 Your feedback for more security

At Avira, our customers' security is paramount. For this reason, we don't only have an in-house team of experts to test the quality and security of every AntiVir solution and every update before the product is released. We also attach great importance to any indications of security-related weaknesses and deal with these openly.

If you think you have detected a security-related weakness in one of our products, please send us an email to vulnerabilities@avira.com.

# Avira AntiVir ISA Server

**Avira GmbH**

Lindauer Str. 21
88069 Tettnang
Germany
Telephone: +49 (0) 7542-500 0
Fax: +49 (0) 7542-525 10
Internet: http://www.avira.com



Issued Q3-2009